UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

FRANKLIN HUGHES, individually and on behalf of all others similarly situated, Plaintiff, v. T-Mobile USA, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Franklin Hughes ("Plaintiff") brings this Class Action Complaint against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to his own actions, his counsel's investigations, and facts that are a matter of public record, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises from Defendant's failure to properly safeguard its customers' highly sensitive personal identifiable information that Defendant collects and maintains. A cyberattack and data breach perpetrated against Defendant T-Mobile (the "Data Breach") resulted in unauthorized access and exfiltration of highly sensitive and personally

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

identifiable information (the "PII") including first and last names, phone numbers, drivers' license information, government identification numbers, Social Security numbers, dates of birth, T-Mobile account PINs, as well as International Mobile Equipment Identity ("IMEI") and International Mobile Subscriber Identifier ("IMSI") information.[1]

2. As a result of the Data Breach, Plaintiff and approximately 53 million former or prospective customers who applied for credit with T-Mobile, 7.8 million current postpaid customers, and 850,000 active prepaid customers (the "Class Members")[2] suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. As a result of T-Mobile's negligence, PII that T-Mobile collected and maintained is now in the hands of data thieves and as such Plaintiff and Class Members are at a significant risk of identify theft, financial fraud, and/or other fraud imminently and for years to come.

4. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits (including unemployment or COVID relief benefits), filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

5. Plaintiff's and Class Members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and its failure to adequately protect the PII of its current, former, and prospective clients.

6. Plaintiff and Class Members have suffered actual and imminent injuries as a

[1] *See T-Mobile Shares Additional Information Regarding Ongoing Cyberattack Investigation*, T-Mobile (Aug. 20, 2021), https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last visited Aug. 22, 2021).

[2] *Id.*

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

direct result of the Data Breach. The injuries suffered by Plaintiff and the proposed Class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the data breach and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to T-Mobile and with the mutual understanding that T-Mobile would safeguard Plaintiff's and Class Members' personal data against theft and not allow access and misuse of their personal data by others; (f) the reasonable value of the PII entrusted to T-Mobile; and (g) the continued risk to their personal data, which remains in the possession of T-Mobile and which is subject to further breaches so long as T-Mobile fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' personal data in its possession.

7. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed and compromised during the Data Breach.

8. Accordingly, Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's negligence and failure to: (i) adequately protect its customer's PII, (ii) warn its current, former, and potential customers of their inadequate information security practices, and (iii) effectively monitor their data systems for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

9. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

PARTIES

10. Plaintiff Franklin Hughes is a citizen of and is domiciled in the state of Ohio.

11. Defendant T-Mobile is a for-profit company incorporated in Delaware with its principal place of business in the State of Washington at 12920 SE 38th St, Bellevue, Washington 98006. T-Mobile is a wireless network operator and the second largest wireless carrier in the United States. It provides wireless voice and data services for approximately 105 million subscribers.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the aggregate amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

13. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in the State of Washington, Defendant has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

A. Defendant's Business

15. T-Mobile is a national telecommunications company that provides wireless voice, messaging, and data services in the United States and around the globe.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

16. T-Mobile claims to have added 7 million new customers and had $45 billion in total revenue in 2019.[3] T-Mobile also claimed that its stock price increased by 23.3% in 2019.[4]

17. According to Defendant, as of the second quarter of 2021, T-Mobile had 104.8 million customers, making it one of the largest telecommunications providers in the world.[5]

18. Upon information and belief, in the ordinary course of doing business, Defendant collects sensitive PII from customers and potential customers such as name, address, phone number, driver's license number, Social Security number, financial information, government identification number, and date of birth.

19. In the course of collecting PII from customers and potential customers, including Plaintiff and Class Members, Defendant promises to provide confidentiality and security for customers' and potential customer's PII, including by promulgating and placing privacy policies on its website.

20. In the T-Mobile Privacy Notice (hereinafter "Privacy Notice"), which is effective as of May 5, 2021 and provided on Defendant's website, Defendant states that "[Customers] trust T-Mobile to connect [customers] to the world every day, and we're working hard to earn a place in [customers'] heart[s]. A big part of that is maintaining [customer] privacy."[6]

21. Further in the Privacy Notice, Defendant promises to protect consumer's PII and that it uses "administrative, technical, contractual, and physical safeguards designed to protect [customer] data while it is under our control."[7]

22. However, Defendant failed to protect and safeguard Plaintiff's and Class Members' PII. In fact, there is no indication that Defendant followed even its most basic promises. For example, T-Mobile does not claim that any of the stolen PII was encrypted, including usernames and passwords.

---

[3] *See Our Story*, T-Mobile, https://www.t-mobile.com/our-story (last visited Aug. 19, 2021).
[4] *Id.*
[5] *See Investor Factbook*, T-Mobile, https://s24.q4cdn.com/400059132/files/doc_financials/2021/q2/NG_TMUS-06_30_2021-EX-99.2.pdf, at p. 6 (last visited Aug. 19, 2021).
[6] *T-Mobile Privacy Notice*, T-Mobile, https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last visited Aug. 19, 2021).
[7] *Id.*

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

B. The Data Breach

23. On or about August 15, 2021, media reports indicated that an anonymous individual posted for sale a collection of data containing 30 million Social Security numbers and driver licenses, pulled from T-Mobile servers on the dark web, for approximately $270,000.[8] The seller claimed to have additional data related to more than 100 million people—all T-Mobile customers.[9]

24. On August 16, 2021, T-Mobile released a statement that a sophisticated cyberattack had enabled "unauthorized access to some T-Mobile data" by cyberthieves and that it had launched an investigation into the Data Breach.[10]

25. On August 17, 2021, T-Mobile released a statement saying that "[while] our investigation is still underway and we continue to learn additional details, we have now been able to confirm that the data stolen from our systems did include some personal information."[11]

26. On August 19, 2021, T-Mobile posted a "Notice of Data Breach" on its website, confirming that: "T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information."[12]

27. Also on August 19, 2019, T-Mobile began texting the following notice, to Class Members, including Plaintiff Hughes:

---

[8] *See* Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, MOTHERBOARD: TECH BY VICE (Aug. 15, 2021), https://www.vice.com/en/article/akg8wg/ tmobile-investigating-customer-data-breach-100-million (last visited Aug. 22, 2021).

[9] *Id.*

[10] T-Mobile Cybersecurity Incident Update, T-Mobile (Aug. 16, 2021), https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021 (last visited Aug. 19, 2021).

[11] *Supra*, note 1.

[12] *See Notice of Data Breach: Keeping You Safe from Cybersecurity Threats*, T-Mobile (Aug. 19, 2021), https://www.t-mobile.com/brand/data-breach-2021 (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

> "T-Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that your debit/credit card information was compromised. We take the protection of our customers seriously. We are taking actions to protect you T-Mobile account and we recommend that you take action to protect you credit."

28. In addition, the initial investigation discovered that "7.8 million current T-Mobile postpaid customer accounts' information appears to be contained in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile."[13]

29. T-Mobile also confirmed that the cyberthieves accessed and stole "customers' first and last names, date of birth, SSN, and driver's license/ID information for a subset of current and former postpay customers and prospective T-Mobile customers[,]" as well as "850,000 active T-Mobile prepaid customer names, phone numbers and account PINs[.]"[14]

30. At this time, Defendant has not indicated how long the unauthorized third-party had unfettered access to sensitive, protected, and confidential customer information stored on Defendant's network, such as Plaintiff's and Class Members' PII. Had Defendant taken its data security obligations more seriously, Defendant would have discovered and stopped the unauthorized intrusion sooner.

31. Upon information and belief, the cyberattack was targeted at Defendant due to its status as a leading telecommunications company that collects and maintains valuable PII, such as Social Security numbers and financial information.

32. The targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of current, former, and prospective customers, like Plaintiff and the Class Members.

33. Because of this targeted cyberattack, data thieves were able to gain access to Defendant's servers and subsequently access and exfiltrate the protected PII of Plaintiff and

[13] *Supra*, note 1.
[14] *Id*.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Class Members.

34. By Defendant's own admission, "we have now been able to confirm that the data stolen from our systems did include some personal information" which means that Plaintiff's and Class Members PII was exfiltrated as well, not merely viewed without authorization.

35. The files accessed by this incident contained the following information: names, dates of birth, phone numbers, drivers' licenses, government identification numbers, Social Security numbers, and T-Mobile account PINs.

36. There is no indication that the PII contained in the stolen files was encrypted.

37. Plaintiff's PII was accessed and stolen in the Data Breach. Plaintiff further believes his stolen PII was subsequently sold on the Dark Web.

38. Defendant's offer of twenty-four months of complimentary credit monitoring services is an acknowledgment by T-Mobile that the impacted individuals are subject to a present and ongoing threat of fraud and identity theft.

39. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

40. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation, and mutual understanding, that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

C. Defendant Has Failed to Secure Customers' Sensitive Data Multiple Times

41. This is not T-Mobile's first data breach, rather this is T-Mobile's fifth data breach in the past three years.

42. As the Washington Post reported, "[u]nfortunately, dealing with data breaches is nothing new for the company — or its customers. For those keeping count, this is the fifth such incident the wireless carrier has suffered in the past three years, but according to Allie Mellen,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

a security and risk analyst at Forrester Research, this is 'the worst breach they've had so far.'"[15]

43. In August 2018, sensitive information for over 2 million T-Mobile customers was exposed.[16] In November 2019, approximately 1 million T-Mobile users' names, addresses, phone numbers, account numbers, rate plans, and customer proprietary network information was accessed by hackers.[17] Less than six months later, in March 2020, an unknown number of customers' names, addresses, phone numbers, account numbers, rate plans and features, and billing information was accessed by hackers.[18] Later that year, the private information of approximately 200,000 customers' data was exposed in yet another breach.[19]

44. Despite its dismal record of protecting its customers' sensitive information, T-Mobile continues to market itself as a sophisticated, reliable network provider that sets itself apart by its "100% customer commitment."[20] T-Mobile represents that "[a]t T-Mobile, privacy and security is of utmost importance," and that the company "take[s] our customer and prospective customer privacy VERY seriously."[21]

45. Even after this Data Breach, T-Mobile continues to say that "Customers trust us with their private information, and we safeguard it with the utmost concern."[22]

---

[15] *T-Mobile Breach Leads To The Exposure Of Employee Email Accounts And User Data*, Identity Theft Resource Center, Mar. 2020, available at https://www.idtheftcenter.org/t-mobile-breach-leads-to-the-exposure-of-employee-email-accounts-and-user-data/#:~:text=On%20Thursday%2C%20March%204%2C%202020%2C%20T-Mobile%20disclosed%20a,separate%20data%20breach%20notification%20letters%20on%20their%20website.

[16] Alicia Hope, *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 subscribers*, CPO MAGAZINE (Jan. 11, 2021), https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/ (last visited Aug. 22, 2021).

[17] Dewin Coldewey, *More than 1 million T-Mobile customers exposed by breach*, TECHCRUNCH (Nov. 22, 2019), https://techcrunch.com/2019/11/22/more-than-1-million-t-mobile-customers-exposed-by-breach/ (last visited Aug. 22, 2021).

[18] T-Mobile's Data Breach Exposes Customer's Data and Financial Information, SECURITY MAGAZINE (Mar. 6, 2020), https://www.securitymagazine.com/articles/91856-t-mobiles-data-breach-exposes-customers-data-and-financial-information (last visited Aug. 19, 2021).

[19] Hope, *supra* note 18.

[20] *Un-Carrier History*, T-MOBILE, https://www.t-mobile.com/our-story/un-carrier-history (last visited Aug. 22, 2021).

[21] John Legere, *A Letter from CEO John Legere on Experian Data Breach*, T-MOBILE (Sept. 30, 2015), https://www.t-mobile.com/news/blog/experian-data-breach (last visited Aug. 22, 2021).

[22] See Notice of Data Breach: Keeping you safe from cybersecurity threat, T-Mobile (last visited August 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

46. T-Mobile was very familiar with its obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

47. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

48. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

49. Data breaches have become widespread. For example, the United States saw 1,244 data breaches in 2018 and had 446.5 million exposed records.[23]

50. Defendant clearly understood this reality because a quote, posted on Defendant's website, by a senior manager of Defendant's Cyber Architecture & Controls unit stated that:

> At T-Mobile, everyone is challenge[d] to think outside of conventional approaches to digital security; all know assumptions are reevaluated. We work on forward-thinking technologies, including micro-segmentation, machine learning, predictive analytics, web situational awareness, advance threat mitigation, active defense, data obfuscation and next-generation endpoint technologies it.[24]

51. However, T-Mobile failed to fully implement data security systems and protect critical PII belonging to consumers.

52. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry,

[23] *98 Must-Know Data Breach Statistics for 2021*, Varonis, https://blogvaronis2.wpengine.com/data-breach-statistics/ (last visited Aug. 19, 2021).

[24] *Digital Security*, T-Mobile, https://www.t-mobile.com/careers/digital-security (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

including Defendant.

53. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[25] Identity thieves use stolen personal information for a variety of crimes, including government benefits fraud, phone or utilities fraud, and bank and finance fraud.[26]

54. The PII of Plaintiff and Members of the Class was taken by hackers to engage in identity theft or to sell to other criminals who will purchase the PII for that purpose, or both. The fraudulent activity resulting from the Data Breach may not come to light for years.

55. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Members of the Class, including Social Security numbers, driver's license, and/or dates of birth, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Members of the Class a result of a breach.

56. Plaintiff and Members of the Class now face years of constant surveillance of their financial and personal records. Plaintiff and Members of the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

57. The injuries to Plaintiff and Members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Members of the Class.

D. Defendant Failed to Comply with FTC Guidelines

58. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need

---

[25] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Aug. 19, 2021).

[26] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

63. Defendant was at all times fully aware of their obligation to protect the PII of current, former, and prospective customers. Defendant was also aware of the significant

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

repercussions that would result from their failure to do so.

E. Defendant Failed to Comply with Industry Standards

64. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

65. Best cybersecurity practices that are standard in Defendant's industry include encrypting files; installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

66. Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

67. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyberattack and causing the Data Breach.

F. Defendant's Breach

68. T-Mobile breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. T-Mobile's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

b. Failing to adequately protect current, former, and prospective customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

e. Failing to adhere to industry standards for cybersecurity.

69. T-Mobile negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

70. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with T-Mobile.

G. The Value of PII to Cyber Criminals and Increased Risk of Fraud and Identity Theft to Consumers

71. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

72. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[27]

73. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are

[27] *See Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[28]

74. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

75. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[29]

76. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to

[28] *Identity Theft and Your Social Security Number*, Social Security Administration (2018); *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 19, 2021).

[29] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

> identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same. If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[30]

77. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and Class Members stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class.

78. Stolen personal data of Plaintiff and Class Members represents essentially one-stop shopping for identity thieves.

79. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

80. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for 16 years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future

[30] *Supra*, note 18.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

harm.[31]

81. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and members of the Classes has a high value on both legitimate and black markets.

82. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment or COVID-19 relief benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

83. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's current, former, and prospective customers whose Social Security numbers have been compromised now face a present and imminent risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

84. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because in that situation victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth.

85. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on

[31] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) at 29, *available at:* https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 19, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

the black market."[32]

86. According to a recent article in the New York Times, cyber thieves are using illegally obtained driver's licenses to submit and fraudulently obtain unemployment benefits.[33] An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

H. The Plaintiff's Experience

Plaintiff Franklin Hughes

87. Plaintiff Franklin Hughes is a customer of T-Mobile.

88. Plaintiff Hughes opened his cellular telephone postpaid customer account with Defendant in or about May 2021. Plaintiff has three lines of service with T-Mobile.

89. Plaintiff was required to provide, among other things, certain private and confidential personal information, including his full name, date of birth and Social Security number for the provision of Defendant's services. Plaintiff was also approved for credit with T-Mobile.

90. T-Mobile obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

91. On or about August 16, 2021, Plaintiff Hughes, and the public, was first notified of the Data Breach by T-Mobile and that cybercriminals had illegally accessed and stole confidential customer data from millions of T-Mobile customer accounts. In addition, Plaintiff Hughes received the August 19, 2021 text message from T-Mobile notifying him that his PII was among the confidential data that cybercriminals illegally accessed and stole from Defendant's servers.

---

[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 19, 2021).

[33] *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021) https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Aug. 19, 2021)

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

92. As a direct and proximate result of the breach, Plaintiff Hughes has made reasonable efforts to mitigate the impact of the breach, including but not limited to: researching the internet concerning this Data Breach; discussing the breach with his family; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. He now plans to spend several hours a month reviewing account statements for irregularities and fraudulent inquiries.

93. Plaintiff Hughes would not have entrusted his personal information to T-Mobile had he known that T-Mobile failed to maintain adequate data security.

94. Plaintiff Hughes is very concerned about identity theft, his banking account and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

95. Plaintiff Hughes suffered actual injury from having PII compromised because of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

96. Plaintiff Hughes has and will spend a significant amount of time responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff otherwise would have spent on other activities.

97. As a result of the Data Breach, Plaintiff Hughes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

98. Since learning about the Data Breach, Plaintiff Hughes has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of his PII.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

I. Plaintiff's and Class Members' Damages

99. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

100. Defendant has only offered inadequate identity monitoring services. Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime. In addition, Defendant only offers these services for two years, even though experts agree that the effects of such a data breach can often be felt by victims for around seven years.

101. Plaintiff's and Class Members' PII were compromised as a direct and proximate result of the Data Breach.

102. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members are in imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

104. Plaintiff and Class Members face a present and substantial risk of out-of-pocket fraud losses such as loans opened in their names, government benefits fraud, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

105. Plaintiff and Class Members face a present and substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

106. Plaintiff and Class Members have and may continue to incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

107. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

108. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts for misuse. Indeed, Defendant's own Notice of Data Breach page posted on its website states that the stolen data is in "harm's way" and encourages Plaintiff and Class Members to "take proactive steps regularly to protect your data and identity[.]"[34]

109. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges, loans, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security numbers, bank accounts, and credit reports for unauthorized activity for years to come.

110. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that

[34] *Notice of Data Breach: Keeping You Safe from Cybersecurity Threats*, T-Mobile (Aug. 22, 2021), https://www.t-mobile.com/brand/data-breach-2021 (last visited Aug. 22, 2021).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

such data is properly encrypted.

111. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future harm.

112. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

113. Defendant has only offered inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach. What is more, Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

CLASS ALLEGATIONS

114. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> **All current, former, and prospective T-Mobile customers residing in the United States whose personally identifiable information ("PII") Information was compromised in the Data Breach (the "Class").**

115. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. and all judges assigned to hear any aspect of this litigation and their immediate family members, as well as any judicial staff.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

116. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

117. Numerosity: The Class is so numerous that joinder of all members is impracticable. Defendant has identified millions of current, former, and prospective customers whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

118. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiff and Members of the Class;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiff and Members of the Class;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the PII of Plaintiff and Members of the Class secure and to prevent loss or misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff and Members of the Class damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and Members of the Class that their PII had been compromised;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

j. Whether Defendant violated the consumer protection statute invoked below; and

k. Whether Plaintiff and the other Members of the Class are entitled to credit monitoring and other monetary relief.

119. Typicality: Plaintiff's claims are typical of those of the other Members of the Class because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

120. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

121. Superiority and Manageability: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

122. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

123. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Members of the

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Class to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Members of the Class to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

124. Plaintiff realleges and incorporates all foregoing factual allegations contained in each of the preceding paragraphs as if fully set forth herein.

125. Defendant owed a common law duty to Plaintiff and Members of the Class to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

126. The legal duties owed by Defendant to Plaintiff and Members of the Class include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Members of the Class in its possession;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

b. To protect PII of Plaintiff and Members of the Class in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Members of the Class of the Data Breach.

127. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

128. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Members of the Class are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

129. Defendant breached its duties to Plaintiff and Members of the Class. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging in the past 5 years.

130. Defendant knew or should have known that its security practices did not adequately safeguard the PII belonging to the Plaintiff and Members of the Class.

131. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and Members of the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Members of the Class during the period it was within Defendant's possession and control.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

132. Defendant breached the duties it owed to Plaintiff and Members of the Class in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect current, former, and prospective customers' PII, including Plaintiff and Members of the Class, and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards prior to the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

133. Due to Defendant's conduct, Plaintiff and Members of the Class are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against Plaintiff and Members of the Class.

134. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.[35]

135. As a result of Defendant's negligence, Plaintiff and Members of the Class suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing scams and reviewing and monitoring sensitive accounts; (iv) the present and continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to

[35] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Members of the Class, including ongoing credit monitoring.

136. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the members of the Class suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II

Negligence Per Se

(On Behalf of Plaintiff and the Class)

137. Plaintiff realleges and incorporates all foregoing factual allegations contained in each of the preceding paragraphs as if fully set forth herein.

138. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

139. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

140. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

141. Plaintiff and Members of the Class are within the class of persons that the FTC Act was intended to protect.

142. The harm that occurred as a result of the Data Breach is the type of harm the

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Members of the Class.

143. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the present and continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of its current, former, and prospective customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Members of the Class.

144. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and Members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

COUNT III

Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

145. Plaintiff realleges and incorporates all foregoing factual allegations contained in each of the preceding paragraphs as if fully set forth herein.

146. Defendant provided Plaintiff and Class Members with an implied contract to protect and keep confidential Defendant's current, former, and prospective customers' private, nonpublic personal and financial information when they gathered the information from each of their current, former, and prospective customers.

147. Plaintiff and Class Members would not have provided their personal and financial information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's current, former, and prospective customers private personal and financial information.

148. Plaintiff and Class Members performed their obligations under the implied contract when they provided their private personal and financial information in exchange for telecommunication services provided by Defendant.

149. Defendant breached the implied contracts with Plaintiff and Class Members by failing to protect and keep private the nonpublic personal and financial information provided to it about Plaintiff and Class Members.

150. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, damages and injuries.

COUNT IV

Violation of the Washington State Consumer Protection Act (RCW 19.86.010 et seq.)

(On Behalf of Plaintiff and the Class)

151. Plaintiff realleges and incorporates all foregoing factual allegations contained in each of the preceding paragraphs as if fully set forth herein.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

152. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

153. Defendant is a "person" as described in RWC 19.86.010(1).

154. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that it engages in selling telecommunication products and services, that directly and indirectly affect the people of the State of Washington.

155. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

156. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PII, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

157. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

158. As a direct and proximate result of Defendant's above-described wrongful

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality their PII; (4) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (5) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

159. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

160. Plaintiff, on behalf of himself and the Class Members also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of himself and the Class Members requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per class member.

COUNT V

Breach of Implied Duty of Good Faith and Fair Dealing

(On Behalf of Plaintiff and the Class)

161. Plaintiff realleges and incorporates all foregoing factual allegations contained in each of the preceding paragraphs as if fully set forth herein.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

162. Plaintiff and Class Members entered into and/or were the beneficiaries of contracts with Defendant, as alleged above.

163. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendant would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and federal and state laws and regulations for the security of this information.

164. Special relationships exist between Defendant and Plaintiff and Class Members. Defendant entered into special relationships with Plaintiff and Class Members, who entrusted their confidential PII to Defendant and paid for services with Defendant.

165. Defendant promised and was obligated to protect the confidentiality of Plaintiff's and Class Members' PII from disclosure to unauthorized third parties. Defendant breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, which resulted in the Data Breach. Defendant unreasonably interfered with the contract benefits owed to Plaintiff and Class Members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the PII of Plaintiff and the Class in Defendant's possession.

166. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant, including paying Defendant for services and providing them the confidential PII required by the contracts.

167. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff and Class Members did not receive the full benefit of their bargain—services with reasonable data privacy—and instead received services that were less valuable than what

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members have suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiff and Class Members paid for, and the services they received without reasonable data privacy.

168. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PII and remain at imminent risk of suffering additional damages in the future.

169. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach, including but not limited to taking steps to protect themselves from the loss of their PII.

170. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class Members suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendant from its conduct. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law.

COUNT VI

Unjust Enrichment

(Alternative to Breach of Contract Claim)

(On Behalf of Plaintiff and the Class)

171. Plaintiff realleges and incorporates all foregoing factual allegations contained in each of the preceding paragraphs as if fully set forth herein.

172. Defendant benefited from receiving Plaintiff's and Members of the Class' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

173. Defendant also understood and appreciated that Plaintiff's and Members of the Class' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

174. Plaintiff's and Members of the Class conferred a monetary benefit upon Defendant in the form of monies paid for services available from Defendant.

175. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Members of the Class.

176. The monies that Plaintiff and Members of the Class paid to Defendant for services should have been used by Defendant, at least in part, to pay for the administrative costs and implementation of reasonable data privacy and security practices and procedures.

177. Defendant also understood and appreciated that Plaintiff's and Members of the Class' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

178. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed Plaintiff and Members of the Class that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

179. As a result of Defendant's wrongful conduct, Defendant was unjustly enriched at the expense of, and to the detriment of, Plaintiff and Members of the Class. Defendant continues to benefit and profit from its retention and use of the PII while the value to Plaintiff and Members of the Class has been diminished.

180. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this Complaint, including compiling, using, and retaining Plaintiff's and Members of the Class' PII, while at the same time failing to maintain that information secured from intrusion and theft by hackers and identity thieves.

181. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the amount Plaintiff and Members of the Class paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

privacy and security practices and procedures.

182. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

183. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and that the Court grant the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and his Counsel to represent the certified Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and class members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

RESPECTFULLY SUBMITTED AND DATED this 23rd day of August, 2021.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759
Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 N. 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 206-816-6603
Facsimile: (206) 319-5450

Bryan L. Bleichner*
Email: bbleichner@chestnutcambronne.com
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300

Justin C. Walker*
Email: jwalker@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
Facsimile: (513) 665-0219

Attorneys for Plaintiff

**Pro hac vice forthcoming*